Manual Pack Seguridad Autónomos

Antivirus + Firewall + Filtrado Web

Manual de Usuario

Antivirus + Firewall + Filtrado Web

ÍNDICE

1. Introducción
2. Características
3. Requisitos del Sistema
4. Instalación
5. Uso
6. Utilidades

1. Introducción

Movistar pone a su disposición el Pack Seguridad Autónomos que incluye las protecciones ***Antivirus + Firewall + Filtrado Web***. Una vez instalado el producto en los equipos de su empresa, la gestión global de los mismos comprobará automáticamente la presencia de amenazas.
Cuando Usted contrata licencias del Pack Seguridad Autónomos está adquiriendo licencias de uso y disfrute que protegen sus equipos.

2. Características

Una vez terminada la instalación inicial en los equipos correspondientes, se ejecuta de forma invisible en el PC y se actualiza automáticamente.

A continuación envía informes al servidor que describen el estado actual de todos los ordenadores de la empresa con información sobre las detecciones de amenazas.

Características básicas de Firewall.

La protección ***Firewall,*** incluida en el servicio, ofrece una protección avanzada para los equipos y los datos personales de los usuarios. Establece una barrera entre el equipo e Internet y controla el tráfico en busca de incidentes sospechosos.

La protección ***Firewall*** presenta las siguientes características:

- Protege frente a posibles exploraciones y ataques de *hackers*
- Complementa las defensas antivirus
- Supervisa Internet y los incidentes de la red
- Alerta de incidentes potencialmente hostiles
- Ofrece información pormenorizada sobre el tráfico sospechoso por Internet
- Ofrece funciones de seguimiento detallado y búsqueda de incidentes.

Características básicas de Antivirus.

La protección ***Antivirus***, incluida en el servicio, ofrece:

- **Protección continua:**
  Vigila en silencio todas las entradas y salidas de archivos, las descargas, las ejecuciones de programas y demás actividades relacionadas con el sistema.

- **Descubrimiento instantáneo:**
  Cuando detecta un virus, trata de desinfectar e l archivo infectado o lo pone en cuarentena. Además, guarda la información de la detección y la transmite al servidor para elaborar informes.

- **Actualización automática:**
  Vigila continuamente el sistema y compara los archivos de definición de virus (DAT) con la versión más reciente. Cuando detecta un DAT nuevo, lo obtiene automáticamente.

- **Sistema de advertencia precoz AVERT:**
  Utiliza la información de amenazas y brotes de virus más recientes descubiertas por los laboratorios AVERT, una división de McAfee, nuestro proveedor de software para este producto.

Características básicas de Filtrado Web.

La protección ***Filtrado Web***, incluida en el servicio, garantiza la protección contra las vulnerabilidades en sitios web para todos los usuarios.

La protección ***Filtrado Web*** presenta las siguientes características:

- Bloquea páginas de Phishing (páginas web falsas destinadas a robar datos confidenciales)
- Permite configurar el acceso a sitios web en función de su clasificación de seguridad general.
- Permite configurar el acceso a descargas de ficheros en función de su clasificación.
- Permite configurar el acceso a sitios web según su categoría de contenido.
- Permite autorizar o bloquear el acceso a sitios web especificados por el administrador.

Otras Características Avanzadas.

La actualización regular es la base del servicio. En una situación simple, cada estación de trabajo se conecta directamente al Centro de Operaciones de Red (NOC) a través de Internet y comprueba si hay nuevas actualizaciones para la protección instalado en los equipos. Varias funciones ayudan a utilizar de forma eficaz los recursos de red; por ejemplo:

- **Actualización independiente de Internet**
  Esta función permite a cualquier ordenador de la red obtener información del NOC, incluso si el ordenador no está conectado a Internet.

  La función de Actualización independiente de Internet permite usar el servicio en ordenadores no conectados a Internet. Para usar esta función, al menos una de las

estaciones de trabajo de la subred debe tener una conexión con Internet capaz de comunicarse con el NOC. Esta estación de trabajo se configura como **Servidor de Transmisión**, y los otros ordenadores se conectan con el NOC por medio de él.
El funcionamiento es el siguiente:

- El **Servidor de Transmisión** descarga un catálogo de actualizaciones desde el NOC cuando así se lo solicita otra estación de trabajo que no ha logrado conectar directamente con el NOC.

- La estación de trabajo sin conexión con Internet descarga las actualizaciones necesarias desde el NOC por medio del **Servidor de Transmisión.**

Encontrará más información sobre la configuración de ordenadores como **Servidor de Transmisión** en el apartado ***Otros Métodos de Instalación.***.

- **Tecnología Rumor**
  Rumor es un proceso por medio del cual una estación de trabajo comparte actualizaciones con otros ordenadores de la red local (LAN), lo que evita que cada ordenador tenga que actualizarse individualmente desde el NOC. Esta función reduce la carga de tráfico de Internet en la red.

  La tecnología Rumor funciona como sigue:

  - Cada estación de trabajo recupera del NOC información de versión sobre el catálogo más reciente. Este catálogo contiene información sobre la versión actual de cada componente del producto de seguridad contratado y se almacena con una firma digital en formato de archivo .CAB

    - Si la versión es la misma que ya tiene la estación de trabajo, el proceso no continúa (la estación tiene las actualizaciones más recientes para el producto).
    - Si la versión es distinta de la que presente en la estación de trabajo, ésta trata de recuperar la más reciente del archivo de catálogo de sus iguales; para ello pregunta a los ordenadores de la LAN si han descargado ya la nueva actualización.

  - La estación de trabajo recupera el catálogo solicitado (directamente desde el NOC o desde uno de sus iguales). Utiliza este archivo de catálogo para determinar si hay nuevos componentes.

  - Si los hay, la estación de trabajo trata de recuperarlos a partir de sus iguales, preguntando a los ordenadores de la LAN si ya han descargado componentes nuevos.

    - En caso afirmativo, recupera la actualización a partir de un ordenador local (las firmas digitales vuelven a comprobarse para verificar si la estación de trabajo consultada contiene un archivo de firmas válido).
    - En caso negativo, la estación de trabajo recupera la actualización directamente desde el NOC.

  - Una vez recuperada la actualización, se extrae el archivo .CAB y se instalan los componentes nuevos.

3. Requisitos del Sistema

Sistemas Operativos.

El servicio se ha diseñado para sistemas operativos Microsoft Windows que se ejecutan en plataformas PC. Se instala y funciona en servidores y estaciones de trabajo con:

- **Procesador:** Intel® Pentium® u otro de arquitectura compatible.
- **Navegador:** Microsoft Internet Explorer 6.0 SP2 o posterior
- **Estaciones de trabajo:** Windows 2000 Professional con Service Pack 3 o posterior, Windows XP Home o Professional (32 y 64 bits), Windows Vista (32 y 64 bits), Windows7 (32 y 64 bits).
- **Servidores:** Windows 2000 Server con Service Pack 3 o superior, Windows 2000 Advanced Server con Service Pack 3 o superior, Windows 2000 Small Business Server con Service Pack 3 o superior, Windows 2003 Standard Server, Windows 2003 Enterprise Server, Windows 2003 Web Edition, Windows 2003 Small Business Server.
- **Requerimientos de RAM:** 512 MB mínimo recomendado (mínimo recomendado 512 MB para servidores y 1 GB para Windows Vista.)

Desinstalación de aplicaciones antivirus anteriores.

El servicio ofrece la más reciente tecnología antivirus. Sin embargo, otras aplicaciones antivirus instaladas en el equipo pueden interferir con las avanzadas características de ***Antivirus***. Cuando varios motores de exploración antivirus tratan de acceder a los mismos archivos del ordenador, interfieren unos con otros.

Si durante la instalación recibe mensajes en el sentido de que en su sistema hay otras aplicaciones antivirus, siga las instrucciones que aparecerán para eliminarlas. La lista siguiente recoge todos los productos que ***Antivirus*** desinstala automáticamente.

McAfee para empresas
Anti-Spyware Enterprise (todas las ediciones)
ePO agent
Managed VirusScan y Managed Desktop Firewall (ediciones anteriores)
Total Protection Enterprise
VirusScan Enterprise 7.0 / 7.1 / 8.0i / 8.5i
VirusScan 4.5.1 para 9x
VirusScan 4.5.1 para NT, 2K, XP
VirusScan 4.5.1 SP1 para 9x
McAfee para usuarios particulares
Internet Security Suite
McAfee SecurityCenter
Total Protection para usuarios particulares
VirusScan Retail 8.0
VirusScan Professional Edition 7.0
VirusScan Home Edition 7.0
VirusScan Professional Edition 6.0
VirusScan Home Edition 6.0

VirusScan Retail 5.1.X
VirusScan Retail 5.0 para 9x
VirusScan Retail-OEM 4.0.3 para 9x

Computer Associates

eTrust AntiVirus 7.1
eTrust AntiVirus 7.0
Inoculate IT 3.5.1
Inoculate IT 4.5.3
Pest Patrol para software espía

Finjan SurfinShield Corporate

F-Secure

AntiVirus 5.52 Antivirus 2004 (home)
Antivirus Client Security (sólo desinstalar antivirus)
F-Secure Internet Security 2006

Kaspersky

AntiVirus Personal
AntiVirus Personal Pro
Antivirus Business Optimal

Norton/Symantec Norton Internet Security 2004 (ediciones "home" y "small ofice"): desinstala el AV
NAV 2006 Internet Security Edition (sólo desinstala el AV)
NAV 2006 (ediciones 'home' y 'small office')
NAV 2006 Professional
NAV 7.6 para Windows para 9x
NAV 7.6 para Windows para NT
NAV 7.5.1
Norton Internet Security 2004 Professional (edic iones 'home' y 'small office') - desinstala el AV
NAV 2004 (ediciones 'home' y 'small office')
Symantec Antivirus 9.0 (small business)
Norton Systemworks 2002 (sólo desinstala el AV)
Symantec Systemworks 2004 (sólo desinstala el AV)
Symantec Antivirus Corporate Edition 8.1
NAV 2004 Internet Security Edition (sólo desinstala el AV)
NAV 2004 Professional
NAV 2000
NAV Anti-Virus Retail 2000
NAV 2001
NAV 2002
NAV 8.0
NAV 7.6 para Windows para 9X, NT
NAV 7.5.1
NAV 7.5
NAV 7.0 Corporate Edition
NAV 5.0 para Windows para 9X, NT
NAV Central Quarantine
NAV Quarantine Console Snap-in
Norton Mobile Update Agent
Norton Mobile Update Distribution Console
Norton Rescue Disk

Panda
AntiVirus 2.0
Platinum Internet Security
Antivirus Platinum 7.0
Titanium Antivirus 2004, 2003, 2002
BusinessSecure AntiVirus (ClientShield es la sección antivirus)
WebAdmin Antivirus
Sophos Sophos Antivirus
Trend Micro
PC-Cillin Internet Security
PC-Cillin 2004
OfficeScan Corporate Edition
Pc-Cillin 2002
OfficeScan
Virusbuster 2001 para 9x y NT
Virusbuster 2000 para 9x y NT
Virusbuster Corporate HTTP Client NT & 2000
Virusbuster Corporate HTTP Client 9x
Virusbuster Corporate FILEbase Client NT & 2000
Virusbuster Corporate FILEbase Client 9x
Trend Micro HouseCall (en línea)

Si tiene algún software antivirus que no está en esta lista o si, por directiva del propio Windows y/o del software antivirus de terceros no se puede desinstalarlo automáticamente, debe desinstalarlo manualmente antes de instalar ***Antivirus***.

Configuración del Navegador.

La ***Protección*** contratada utiliza el módulo de software *ActiveX* para instalarse y ejecutarse en una estación de trabajo. Los usuarios de Internet Explorer tienen la tecnología *ActiveX* incorporada en sus navegadores. Si decide utilizar otro navegador web como navegador principal, también deberá tener Internet Explorer.

Acerca de *ActiveX*
Un control *ActiveX* es un módulo de software basado en la arquitectura Component Object Model (COM) de Microsoft. Permite a un programa añadir funciones llamando a componentes prefabricados que se combinan entre sí y actúan como si formasen parte del programa.

Internet Explorer 6.0 o superior
El ***Producto*** se ha diseñado para funcionar con la configuración de seguridad predeterminada de Internet Explorer. Esto mantiene la máxima seguridad al tiempo que permite la descarga e instalación de componentes *ActiveX*.

Si no está seguro de la configuración, siga estos pasos para modificar la seguridad de Internet Explorer:

1. En la barra de tareas de Windows, haga clic en el botón **Inicio** y a continuación seleccione **Configuración** y **Panel de control.**
2. Haga doble clic en el icono **Opciones de Internet.**

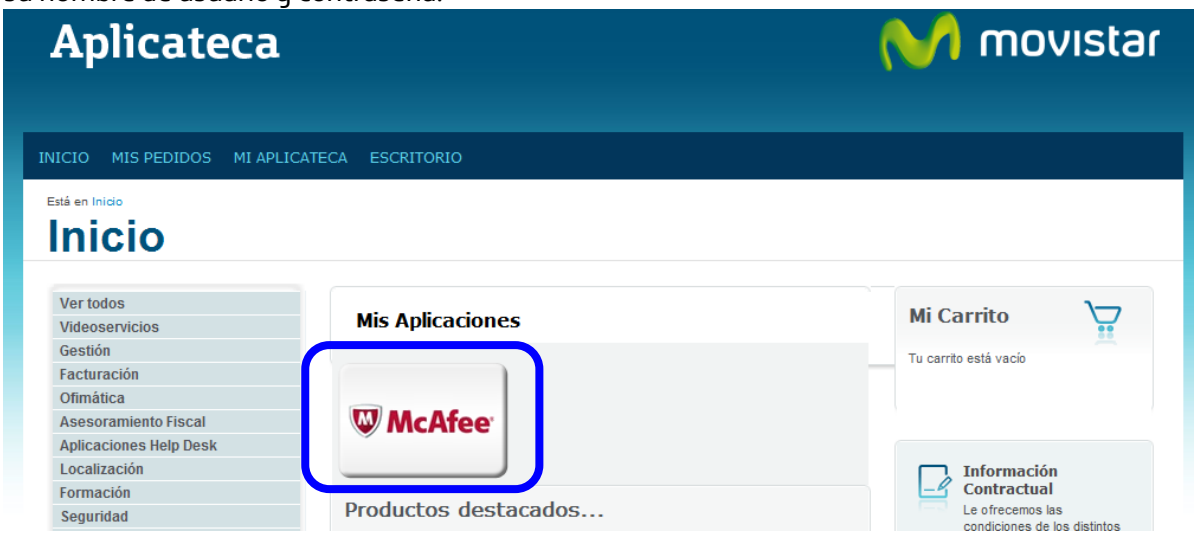
3. Seleccione la ficha **Seguridad.**
4. Haga clic en **Nivel personalizado.**
5. Seleccione **Restablecer a Media** en el menú desplegable. Haga clic en **Restablecer.**
6. Haga clic en **Aceptar** para guardar la configuración.
7. Haga clic en **Aceptar** para salir de Opciones de Internet.

Nota: Aunque sea obligatorio instalar el producto desde una ventana de Internet Explorer, el cliente podrá utilizar otro navegador para abrir las páginas web.

4. Instalación

Una vez comprobado los requisitos del sistema en el apartado anterior, guarde todo el trabajo y cierre todas las aplicaciones abiertas antes de instalar el producto. Después de instalar el Pack debe reiniciar el ordenador.

Para gestionar su Pack Seguridad Autónomos, deberá iniciar sesión en el portal de Aplicateca con su nombre de usuario y contraseña.



Una vez iniciada la sesión, deberá ir al apartado **Mis Aplicaciones**, a continuación hace clic en el botón correspondiente al Pack Seguridad Autónomos contratado. Le aparecerá una nueva ventana como la siguiente:

Con las siguientes pestañas:

· **Informes** con los apartados: “Panel”, “Equipos”, “Informes” y “Directivas”. Para mayor información sobre generación de informes se puede consultar el *capítulo 4 Uso.*

· **Instalación,** Con varios apartados:
“Mis Servicios” donde podrá iniciar la instalación en local o recuperar la URL de instalación directa para facilitarle la misma en otros equipos.

“Instalación Común”, “Instalación Silenciosa”, e “Instalación Remota”.
Con distintos métodos de instalación así como utilidades que pueden ser necesarias dependiendo del equipo elegido.

· **Utilidades**, donde podrá disponer de las siguientes herramientas:

"ContraVirus (Stinger)" realiza un análisis específico para una serie de virus, troyanos y variantes.

"Diagnóstico (MerTool)" Herramienta de Escalación Mínima(herramienta necesaria para abrir una incidencia técnica, permite compilar datos de la configuración del equipo)

"Desinstalador" (herramienta que elimina componentes de Antivirus y/o Firewall de instalaciones anteriores que hayan quedado en el equipo).

INFORMES
INSTALACIÓN
UTILIDADES
DESCONECTAR
Pack Seguridad
...¿necesitas ayuda?
Escaneo rápido (FreeScan)
ContraVirus (Stinger)
Diagnóstico (MER Tool)
CD de arranque (Clean Boot)
Desinstalador
Escaneo rápido (FreeScan) - Escanear Ahora
Escaneo rápido (McAfee FreeScan) le ayuda a detectar miles de virus en su equipo. Basado en el galardonado motor de McAfee VirusScan, busca virus, entre los que se incluyen los últimos virus detectados, y muestra una lista detallada de los archivos infectados. Si se encuentran virus, Escaneo rápido (FreeScan) incluso proporciona vínculos para que tenga más información acerca de los virus y de lo que puede hacer para limpiar el sistema.
aviso legal
protección de datos
grupo Telefónica
Telefónica en el mundo
Telefónica
McAfee
© telefonica.es

Como continuación del proceso de instalación:

1. Localice el apartado **Panel** de la pestaña **Informes** y seleccione botón **Instalar protección** y pulse aquí para iniciar la instalación.

2. A continuación pulse **Instalar protección en este equipo.**

3. Se iniciará el asistente de instalación que le pedirá introducir una dirección de correo electrónico o identificador. Pulsar **Continuar**.

4. Haga clic en **Siguiente** para continuar con la instalación.

5. Si el asistente de instalación se lo pide, haga clic en **Reiniciar** para reiniciar el ordenador. Se abrirá un cuadro de diálogo de bienvenida en cuanto vuelva a arrancar Windows después de la instalación.

Otros Métodos de Instalación.

Dispone de otros métodos de instalación válidos para su máquina u otros equipos si ha ampliado licencias. Los métodos son:

· **Instalación vía URL.** En el Apartado **Mis Servicios** pulsar en **Recuperar URL de Instalación**.

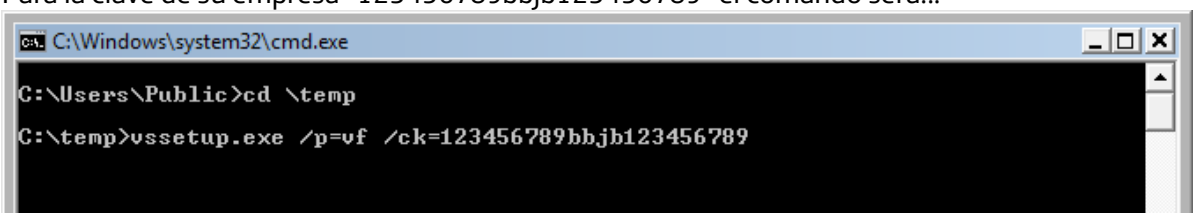
· **Instalación silenciosa.**

Pulsar sobre VSSETUP para Descargar el paquete de instalación. Se abrirá una ventana. Elegir la opción "Guardar", deberá guardar el fichero en una carpeta, por ejemplo C:\Temp.\

Abrir una ventana de Símbolo de Sistema (Hacer clic en el Botón Inicio de Windows => Hacer clic en Ejecutar => En el campo "Abrir", entrar con el comando cmd => Hacer clic en el botón Aceptar). En la ventana de Símbolo de Sistema, deberá ir a donde se encuentra el fichero VSSETUP.EXE , en el ejemplo C:\Temp.\ (con el comando cd \temp) y confirmar con la tecla <Intro>.

Para ejecutar la instalación escriba el comando vssetup.exe /p=VF /ck=xxxxxxxxxxxxxx (deberá reemplazar las xxxxxxxxxxxxxx por los números de su clave de su empresa).

Ejemplo:
Para la clave de su empresa "123456789bbjb123456789" el comando será...



La siguiente es una lista de parámetros de línea de comando que harán que su instalación funcione de forma apropiada.

VSSETUP.EXE	Si se ejecuta VSSETUP.EXE sin parámetros, se abrirá una ventana emergente informando que tiene que usar el parámetro "Company Key" y otros parámetros adicionales.
VSSETUP.EXE /CK=XYZ /P=V	Instalación Silenciosa de **Antivirus** . Donde XYZ es la "Company Key" que se le mandó por correo.
VSSETUP.EXE /CK=XYZ /P=F	Instalación Silenciosa de **Firewall** . Donde XYZ es la "Company Key" que se le mandó por correo.
VSSETUP.EXE /CK=XYZ /P=VF	Instalación Silenciosa de **Antivirus** y **Firewall** . Donde XYZ es la "Company Key" que se le mandó por correo.
VSSETUP.EXE /Email=x@y.com	Este especifica la dirección de correo usada para identificar el usuario del equipo en los informes del Centro de Seguridad
VSSETUP.EXE /Uninstall	Este parámetro hace que se desinstalen **Antivirus** y/o **Firewall** .
VSSETUP.EXE /InstallService	Este instala el módulo "Silent Install package" como un servicio donde al arranque del servicio, tendrá lugar la instalación.
VSSETUP.EXE /UninstallService	Este otro parámetro desinstala el módulo "Silent Install package" del Asistente de Control de Servicios.

Confirmar con la tecla <Intro> para que se ejecute la instalación silenciosa del producto.

Aguarde unos 30 segundos y confirme que el icono/escudo de la Protección aparece en la barra de Tareas de Windows.

CONFIGURANDO UN EQUIPO COMO SERVIDOR DE TRANSMISIÓN

IMPORTANTE: El equipo que servirá de servidor de transmisión debe tener el producto previamente instalado (véase apartado Instalación) y se debe poder navegar por Internet..

1) Descargue el ejecutable **vssetup.exe** al igual que en el procedimiento de instalación silenciosa.
   Abrir una ventana de Símbolo de Sistema (Hacer clic en el Botón Inicio de Windows => Hacer clic en Ejecutar => En el campo "Abrir", entrar con el comando cmd => Hacer clic en el botón Aceptar). En la ventana de Símbolo de Sistema, deberá ir a donde se encuentra el fichero VSSETUP.EXE , en el ejemplo C:\Temp.\ (con el comando cd \temp) y confirmar con la tecla <Intro>.

2) Enseguida deberá introducir el siguiente comando:
vssetup /setrelayserverenable=1

Confirme con la tecla <Intro>. Si ejecuta el comando correctamente, no le aparece ningún mensaje de error. Espere 30 segundos y reinicie el PC.

· **Instalación remota.**

Para más detalles sobre cada uno de los métodos pulse en el enlace que se encuentra en el recuadro Instalación.

5. Uso

Tipos de Usuario:

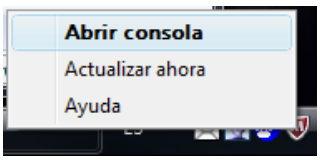
El cliente puede definir distintos tipos de usuario con distintos permisos. Normalmente es aconsejable definir la figura de un usuario **administrador,** aquel que tiene todos los permisos para gestionar, crear y modificar políticas y directivas de seguridad.

Por otro lado está la figura del **usuario** del equipo cuyos permisos son asignados por el usuario **administrador**. Como opciones, puede darle permiso total o por el contrario hacer que este usuario no tenga decisión alguna sobre acciones a realizar.

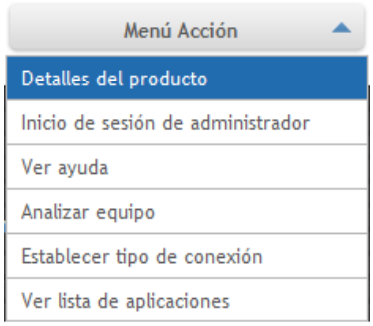
- **Administrador.** Aquel que tiene todos los permisos y asigna los correspondientes al resto.
- **Usuario del equipo.** Aquel cuyos permisos han sido designados por el administrador.

Uso de Firewall.

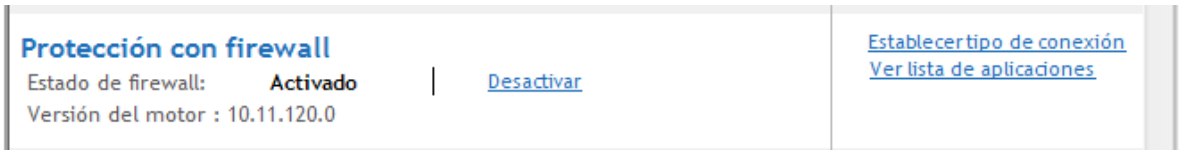
Haga clic en el botón secundario del icono-escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**



Desplegar **Menú Acción** y pulsar sobre **Detalles del producto,**



A continuación, las principales características que puede definir un usuario del equipo en Firewall:



- Estado de Firewall: Activado o Desactivado. Seleccione Activado.

- Establecer tipo de Conexión:

- **Red fiable** (el equipo no puede comunicarse con otros equipos de la red local. Determinados servicios, especificados por el administrador, pueden tener acceso a Internet). Seleccione este tipo de conexión si está conectado indirectamente en una red separada de Internet por un cortafuegos o enrutador de hardware (*Router*). Por ejemplo: en una red doméstica o en la de la oficina.
- **Red No fiable** (el equipo no puede comunicarse con otros equipos de la red local o de Internet). Seleccione esta conexión si está conectado directamente a Internet en, por ejemplo: a través de una conexión de marcación, una línea ADSL o un cable módem; mediante un tipo de conexión en un cibercafé, hotel o aeropuerto.
- **Personalizada** (el equipo sólo puede comunicarse con aquellas direcciones IP y servicios especificados por el administrador). Seleccione esta opción si sólo debe permitir las comunicaciones desde servicios del sistema a través de puertos específicos o desde un rango específico de direcciones IP, o bien si se trata de un servidor que proporciona servicios del sistema. Seleccione su caso y pulse aceptar. Las siguientes aplicaciones, hasta que las defina cualquier tipo de usuario, están permitidas:

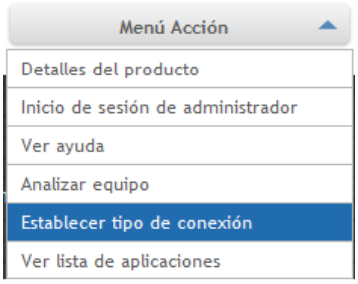
  MYAGTSVC (Agente Rumor)
  UPDDLG (Actualizar motor)
  MCUPDATE (Actualizar agente Virus Scan)
  MSTASK (SO Windows)
  MSDTC (SO Windows)
  SERVICES (SO Windows)
  RPCSS (SO Windows)
  TCPSVS (SO Windows)

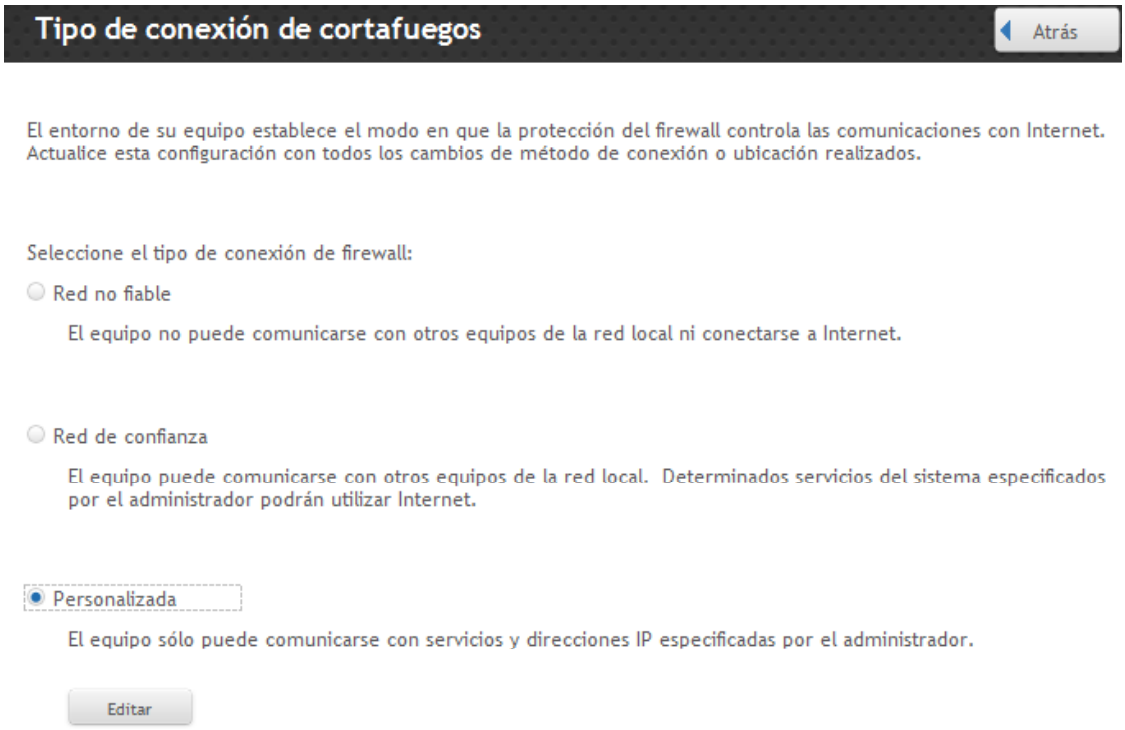
  Cualquier otra aplicación que trate de establecer una conexión a la red será bloqueada.

Configuración personalizada de Firewall.

- Configuración de una conexión personalizada:

Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
Desplegar **Menú Acción** y pulsar sobre **Establecer tipo de conexión,**




Tipo de conexión de cortafuegos
Atrás
El entorno de su equipo establece el modo en que la protección del firewall controla las comunicaciones con Internet. Actualice esta configuración con todos los cambios de método de conexión o ubicación realizados.
Seleccione el tipo de conexión de firewall:
Red no fiable
El equipo no puede comunicarse con otros equipos de la red local ni conectarse a Internet.
Red de confianza
El equipo puede comunicarse con otros equipos de la red local. Determinados servicios del sistema especificados por el administrador podrán utilizar Internet.
Personalizada
El equipo sólo puede comunicarse con servicios y direcciones IP especificadas por el administrador.
Editar

Seleccionar **Personalizada** y pulsar botón **Editar.**

El proceso de personalización permite designar lo siguiente:

- **Equipos que pueden conectarse al suyo:**
  - Cualquier equipo.
  - Mi subred.
  - Intervalo IP específico. Direcciones IP a través de las que el equipo puede recibir las comunicaciones, lo que permite limitar comunicaciones a determinadas direcciones IP.

Agregar servicio aprobado
Seleccione a partir de los servicios conocidos:
Nombre
Web Server (HTTP) Port 80
Universal Plug and Play (UPNP) Port 5000,1900,2869
Microsoft SQL Server (MSFT SQL) Port 1433
Mail Server (SMTP) Port 25
Especifique el nombre del servicio del sistema. Identifique el puerto y el protocolo que se usará para comunicarse con Internet.
Nombre
Puerto
para:
Protocolo
TCP
Aceptar
Cancelar

- **Configurar Conexiones:** (Agregar – Quitar servicio aprobado)

  - Especificar Puertos a través de los que el equipo puede recibir las comunicaciones, necesario para configurar el equipo como un servidor que proporciona servicios del sistema. El equipo aceptará las comunicaciones a través de un puerto abierto del equipo.
  - Se pueden agregar servicios a partir de una lista de servicios conocidos.

- **Seleccione un puerto de los servicios del sistema sólo sí está seguro de que debe abrirse. No es muy habitual que necesite abrir un puerto. Se recomienda desactivar los servicios del sistema sin uso para evitar intrusiones.**
  A continuación se presentan ejemplos de servicios del sistema que generalmente necesitan que los puertos se abran:
  · Servidor de correo electrónico: no es necesario abrir el puerto del servidor de correo para recibir los mensajes de correo electrónico. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de cortafuegos actúa como un servidor de correo.
  · Servidor web: no es necesario abrir un puerto del servidor web para ejecutar un navegador web. Es necesario abrir un puerto sólo si el equipo protegido por el servicio de protección de cortafuegos actúa como un navegador web.

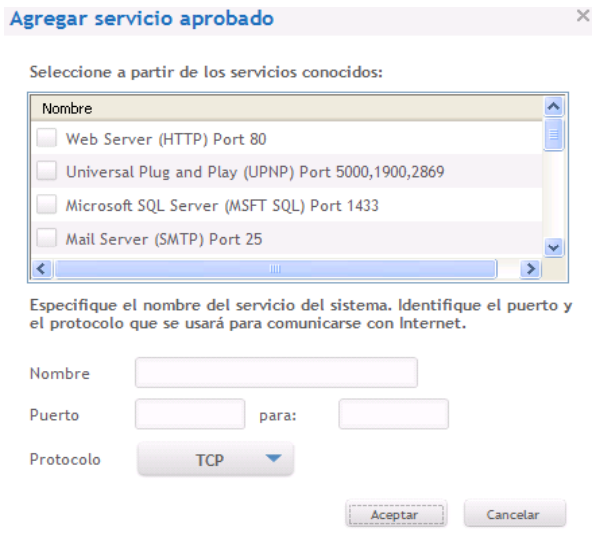
- **Puertos de servicios del sistema.**
  Los servicios del sistema se comunican con Internet a través de los *puertos*, que constituyen conexiones lógicas. Los servicios habituales del sistema de Windows se relacionan generalmente con *puertos de servicio* particulares, y el sistema operativo del equipo u otras aplicaciones del sistema pueden intentar abrirlos. Teniendo en cuenta que estos puertos pueden suponer una fuente de intrusiones para el sistema, debe abrirlos en la configuración predeterminada antes de que equipos externos pueden acceder a ellos. Estos puertos de servicio estándar utilizados habitualmente se enumeran de manera predeterminada en el cuadro de diálogo **Agregar servicio aprobado**, donde puede abrirlos y cerrarlos:

· Puerto 80 del servidor web (HTTP);
· Puerto 5000, 1900, 2869 de Plug and Play universal (UPNP);
· Puerto 1433 de Microsoft SQL Server (MSFT SQL);
· Puerto 25 del servidor de correo (SMTP);
· Puerto 443 del servidor web seguro (HTTPS);
· Puerto 135 de llamadas de procedimiento remoto (RPC, Remote Procedure Calls);
· Puerto 3389 de Remote Assistance/Terminal Server (RDP);
· Puerto 110 del servidor de correo (POP);
· Puertos Comunes Sistemas Operativos (Commom Operating System Ports);
· Puerto 123 de Network Time Protocol;
· Puertos 137-139 de Windows File Sharing (NETBIOS);
· Puerto 143 del servidor de correo (IMAP);
· Puertos 20-21 del protocolo de transferencia de archivos (FTP, File Transfer Protocol);
· Puerto 445 de Microsoft Directory Server (MSFT DS);

Los puertos que no aparecen en la lista del cuadro de diálogo **Agregar servicio aprobado** no están supervisados por el servicio de protección de cortafuegos. Se permitirán las comunicaciones a través de los puertos que no aparecen en la lista. Para bloquear un puerto, debe añadirlo a esta lista y asegurarse de que se ha cancelado su selección.

- **Adición y Edición de puertos del servicio del sistema.**

1. Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
2. Desplegar **Menú Acción** y pulsar sobre **Establecer tipo de conexión.**
3. Seleccionar **Personalizada** y pulsar botón **Editar.**
4. Pulsar **Agregar servicio aprobado.**


Agregar servicio aprobado
Seleccione a partir de los servicios conocidos:
Nombre
Web Server (HTTP) Port 80
Universal Plug and Play (UPNP) Port 5000,1900,2869
Microsoft SQL Server (MSFT SQL) Port 1433
Mail Server (SMTP) Port 25
Especifique el nombre del servicio del sistema. Identifique el puerto y el protocolo que se usará para comunicarse con Internet.
Nombre
Puerto
para:
Protocolo
TCP
Aceptar
Cancelar

5. Especifique el nombre del servicio.
6. Especifique el puerto o puertos a través de los que este servicio se comunicará. (cuando se trate de solo un puerto, hay que ponerlo en ambas casillas)
7. Seleccione el protocolo ("idioma") que el servicio utiliza para establecer la comunicación. Consulte la documentación de la aplicación si no está seguro de el protocolo que debe seleccionar.

TCP: el protocolo de control de transmisión/protocolo de Internet es el protocolo

de Internet más común y se puede utilizar como protocolo de red.
UDP: el protocolo de datagramas de usuario es menos sólido que el TCP. Se utiliza habitualmente para intercambiar pequeñas unidades de datos entre el equipo de una red que utiliza el protocolo de Internet.
Ambos: TCP y UDP.

Nota: si la documentación de la aplicación no especifica el protocolo, se recomienda seleccionar TCP, ya que se trata del protocolo más utilizado. No seleccione Ambos si no se precisan los dos protocolos, ya que, de esta manera, la red será más vulnerable a las intrusiones.

8. Haga clic en **Aceptar**.
9. Una vez agregado se guardan los cambios pulsando **Atrás** o cerrando la ventana.

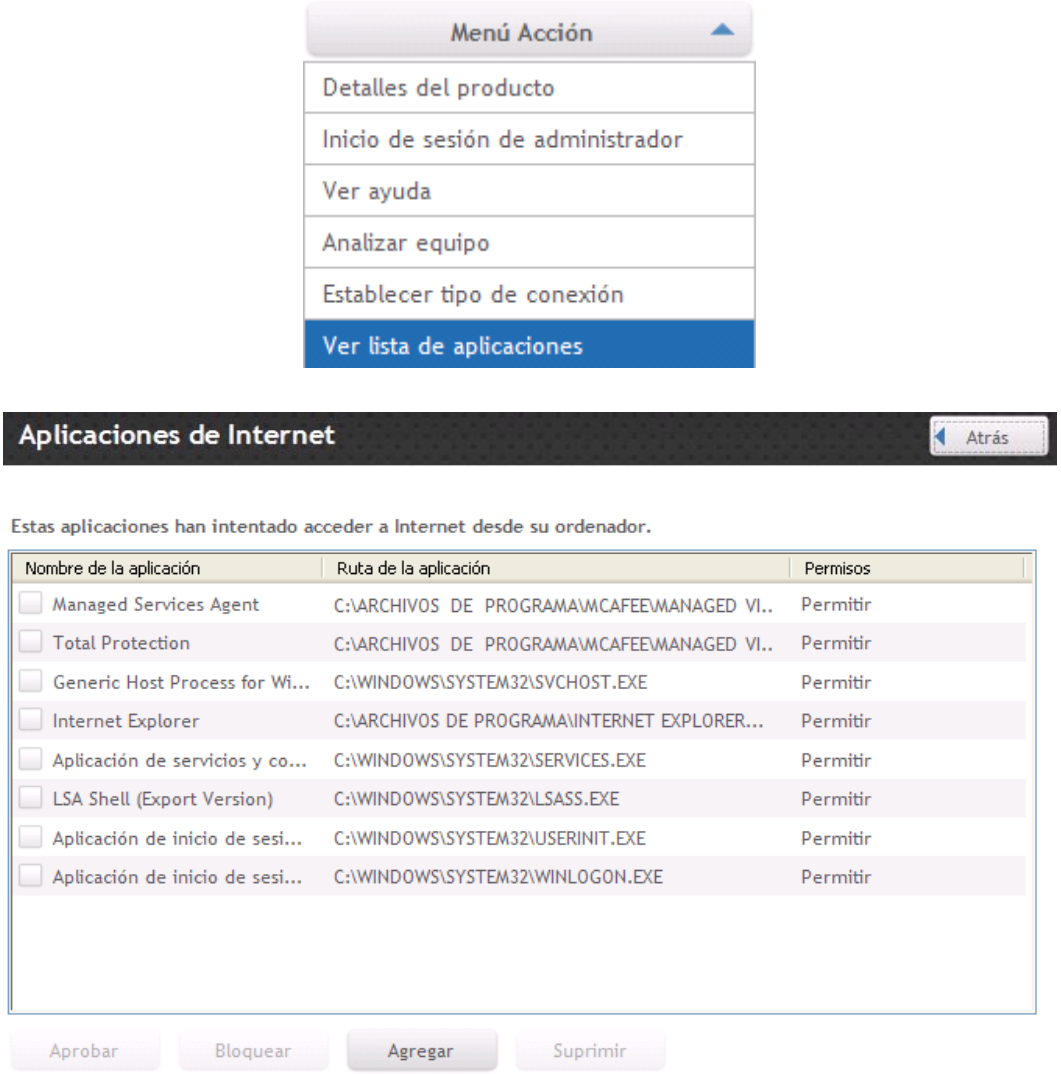
- **Para cerrar un puerto de servicio.**

1. Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
2. Desplegar **Menú Acción** y pulsar sobre **Establecer tipo de conexión.**
3. Seleccionar **Personalizada** y pulsar botón **Editar.**

4. En el recuadro , seleccione un servicio de la lista y, a continuación, haga clic en **Quitar el servicio de la lista.**
5. Se guardan los cambios pulsando **Atrás** o cerrando la ventana.

- Gestión de Aplicaciones de Internet:

1. Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
2. Desplegar **Menú Acción** y pulsar sobre **Ver lista de aplicaciones**



Firewall supervisa las comunicaciones con las aplicaciones de Internet, que se conectan con Internet y su equipo. Cuando la protección de cortafuegos detecta una aplicación de Internet que se ejecuta en el equipo, permite que la aplicación se conecte a Internet o bloquea la conexión, en función de la configuración.

El usuario administrador puede configurar el servicio de protección de cortafuegos para permitir o bloquear determinadas aplicaciones de Internet, además de para solicitarle una respuesta siempre que se detecte una aplicación de Internet

¿Como responde ante una detección?

Cuando la protección de cortafuegos detecta una aplicación de Internet:
1. Comprueba la lista de aplicaciones que se han detectado en el equipo.
2. Comprueba la lista de aplicaciones que se han aprobado
3. Comprueba la "lista blanca" que se mantiene en el sitio www.hackerwatch.org de McAfee.
4. Si la directiva lo permite, le solicita una respuesta; de lo contrario, bloquea la aplicación

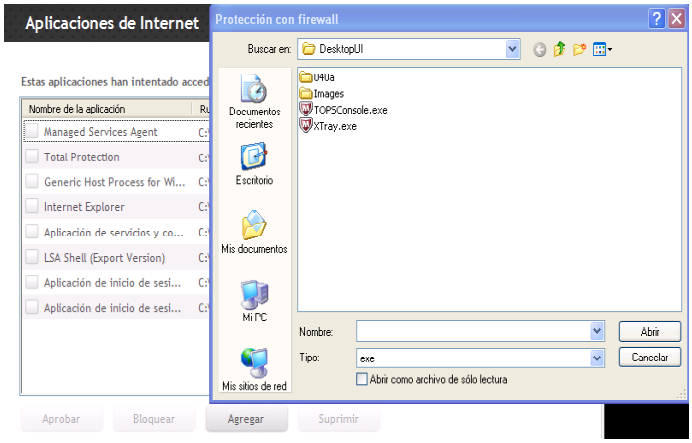
¿Cómo puedo gestionar las aplicaciones de Internet detectadas?

El servicio de protección de cortafuegos mantiene una lista de las aplicaciones de Internet que se

han detectado en el equipo y que ha aprobado. Si la directiva así lo permite, podrá ver estas aplicaciones y sus permisos asignados. También puede cambiar los permisos o suprimir las aplicaciones de la lista.

- **Para gestionar las aplicaciones de Internet:**
  1. Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
  2. Desplegar **Menú Acción** y pulsar sobre **Ver lista de aplicaciones**
  3. Seleccione una aplicación o varias.
  4. Para modificar los permisos de la aplicación:
  - Seleccione **Aprobar** para permitir que la aplicación se comunique con Internet.
  La aplicación aparecerá en los informes administrativos como una aplicación aprobada por el usuario (también conocida como exclusión).
  - Seleccione **Bloquear** para evitar que la aplicación se comunique con Internet.
  - Seleccione **Suprimir** para borrar la aplicación de la lista. La próxima vez que la aplicación trate de acceder a Internet, se le considerará una detección nueva, lo que quiere decir que la directiva determina la respuesta: la protección de cortafuegos bloquea la aplicación, solicita una respuesta o sólo registra el intento.
  5. Se guardan los cambios pulsando **Atrás** o cerrando la ventana.

- **Agregar una Aplicación a la lista.**
  1. Haga clic en el botón secundario del icono/escudo de la Protección situado en la bandeja de sistema y, a continuación, seleccione **Abrir consola.**
  2. Desplegar **Menú Acción** y pulsar sobre **Ver lista de aplicaciones**
  3. Pulsar **Agregar**. Se abrirá el explorador:



  4. Seleccione la aplicación para permitirle la salida a Internet.
  5. Se guardan los cambios pulsando **Atrás** o cerrando la ventana.

Uso de Antivirus.

¿Cómo funciona por defecto *Antivirus*?

La configuración predeterminada del ***Antivirus*** es explorar todos los archivos y carpetas del ordenador cada vez que se acceda a ellos. Los mensajes de correo electrónico no se exploran cuando se reciben, sino en el momento de abrirlos. El responsable de la configuración del analizador en tiempo real es el propio fabricante del producto de ***Antivirus***.

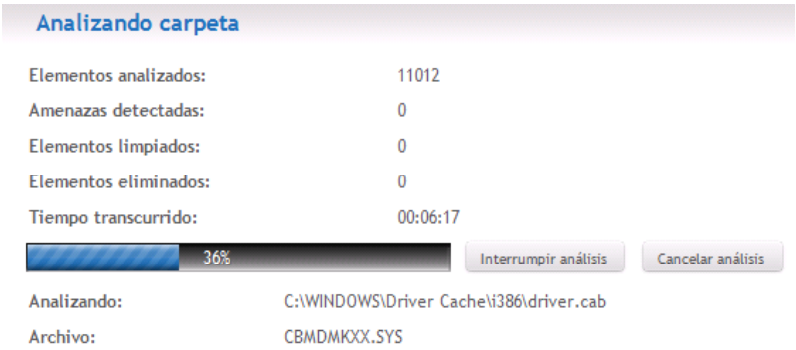
¿Puedo Analizar una unidad o carpeta cuando yo desee?

Sí, con la función **Analizar ahora.**

La función **Analizar ahora** permite explorar una unidad o carpeta determinadas en cualquier momento. Para especificar una exploración:

1. Haga clic con el botón derecho del ratón sobre la Unidad de disco o Carpeta específica y seleccione **Analizar ahora**.

2. Se abrirá la ventana de Análisis:



3. Al finalizar el Análisis, Puede cerrar la ventana o hacer clic en **Ver Informe Detallado** para obtener más información.

   El Informe Detallado del Análisis presentará los siguientes datos:

   Fecha/hora de inicio de la exploración, tiempo de exploración, nivel de actualización de *Antivirus*, fecha de la última actualización, elementos explorados y número de

infecciones detectadas, lista de archivos infectados si los hubiera inclusive previo a la adquisición del producto en su PC.

Para la lista de archivos la situación puede ser una de las siguientes:

- Infectado: el archivo sigue infectado y reside en el sistema. Lo más probable es que el archivo infectado se encuentre dentro de un archivo comprimido (por ejemplo, un ZIP) o se encuentre en un medio protegido frente a escritura.

- Limpio: el archivo se ha limpiado de la infección.

- Limpieza fallida: el archivo no se ha podido limpiar; por tanto, se ha borrado.

Uso de Filtrado Web.

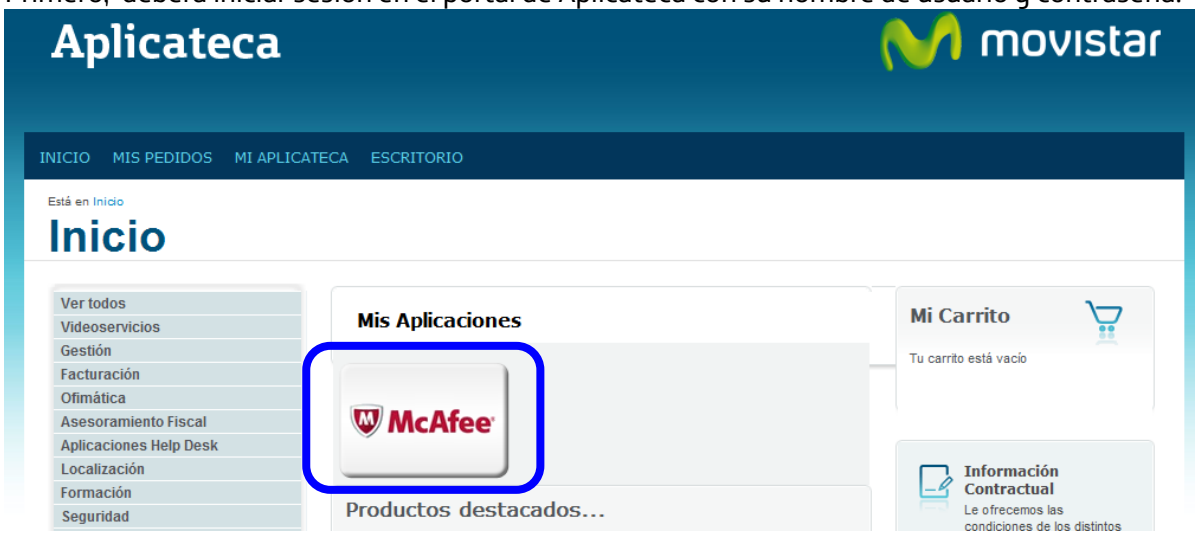
¿Cómo funciona por defecto *Filtrado Web*?

La configuración predeterminada del módulo ***Filtrado Web*** es bloquear el acceso a las páginas de Phishing y sitios web clasificados con "rojo", es decir, aquellos especialmente peligrosos para la seguridad del equipo, por ejemplo, los sitios web que contienen ficheros con virus u otras amenazas, códigos web maliciosos, páginas que envían correos masivos a las direcciones introducidas en sus formularios, etc.

En la directiva predeterminada no se puede configurar el nivel de acceso a sitios web de una categoría de contenido, por ejemplo, bloquear sitios web de chat, juegos, software ilegal, P2P/Uso compartido de ficheros, actividades criminales, etc. Para personalizar la configuración de ***Filtrado Web***, es necesario crear una nueva directiva de seguridad desde el Centro de Seguridad.

¿Cómo puedo crear y personalizar el *Filtrado Web*?

Primero, deberá iniciar sesión en el portal de Aplicateca con su nombre de usuario y contraseña.



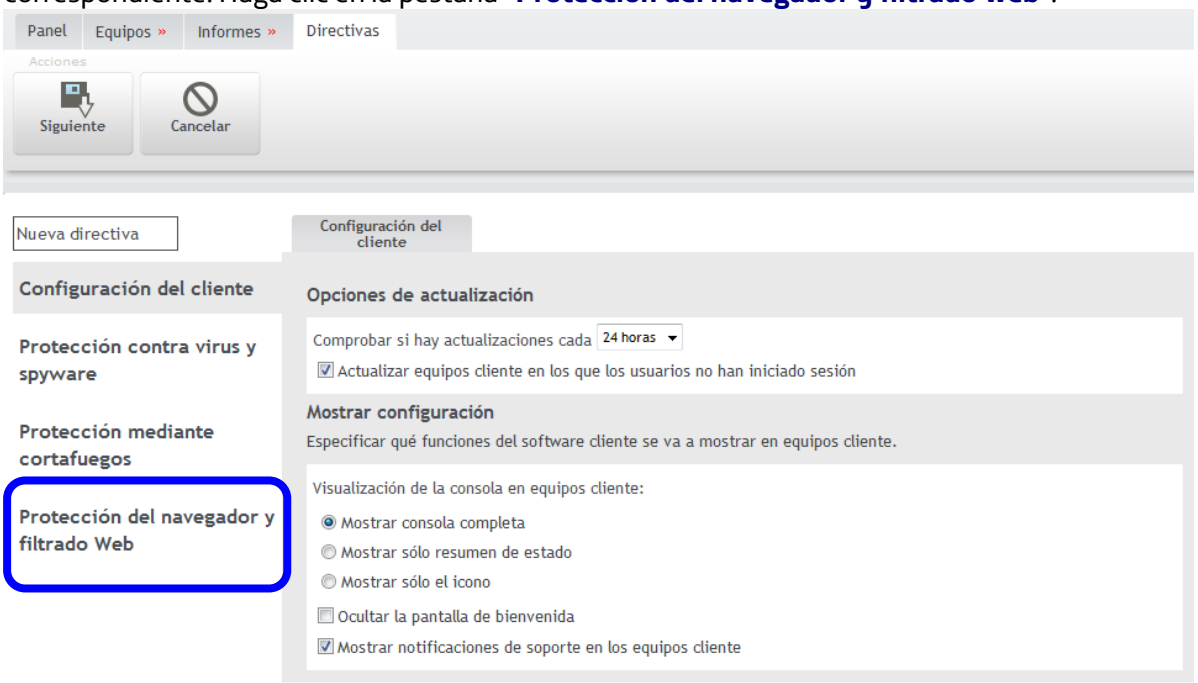
Una vez iniciada la sesión, deberá ir al apartado **Mis Aplicaciones**, a continuación haga clic en el botón correspondiente al Pack Seguridad contratado. Le abrirá una nueva ventana como la siguiente:

A continuación, haga clic en la pestaña "**Directivas**".

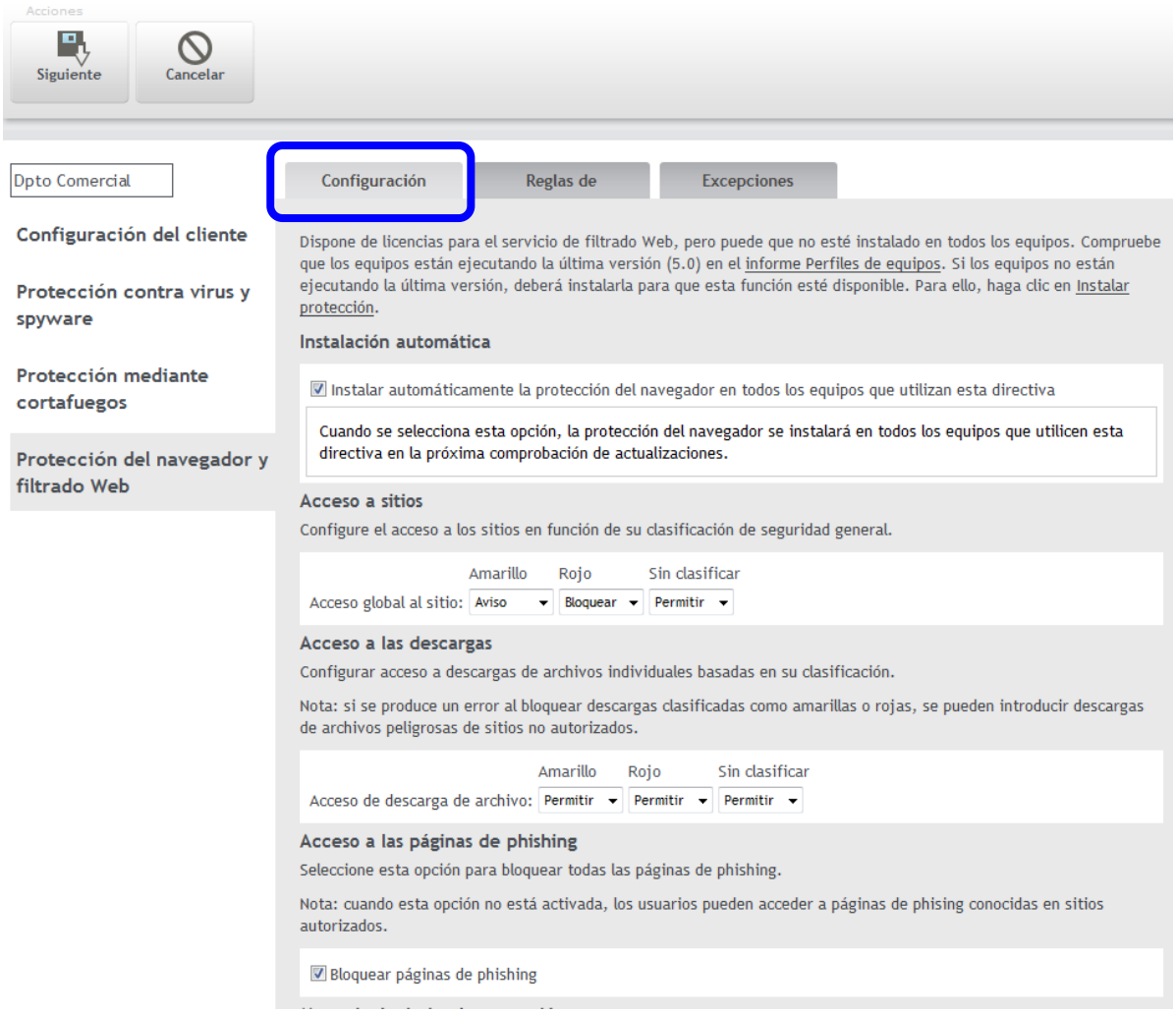
En el apartado “**Directivas**”, haga clic en el botón “Agregar Directivas”.

Centro de Seguridad
movistar
INFORMES / INSTALACIÓN / UTILIDADES / DESCONECTAR
Pack Seguridad
...¿necesitas ayuda?
Panel
Equipos »
Informes »
Directivas
Agregar Directiva
Directiva predeterminada:
McAfee Default
Nombre de directiva
Equipos
Acciones
McAfee Default
0
Ver directiva
ricardo
0
Editar | Eliminar | Copiar directiva
Aviso legal: La protección frente a virus y spyware está configurada de forma predeterminada para detectar programas potencialmente no deseados como, por ejemplo, el spyware. Seleccione si desea mantener o cambiar esta configuración de detección. En algunos casos, la eliminación de estos programas puede provocar que los programas host no funcionen correctamente, exigir que se desinstalen otros programas con acuerdo de licencia o requerir alguna otra acción por su parte.

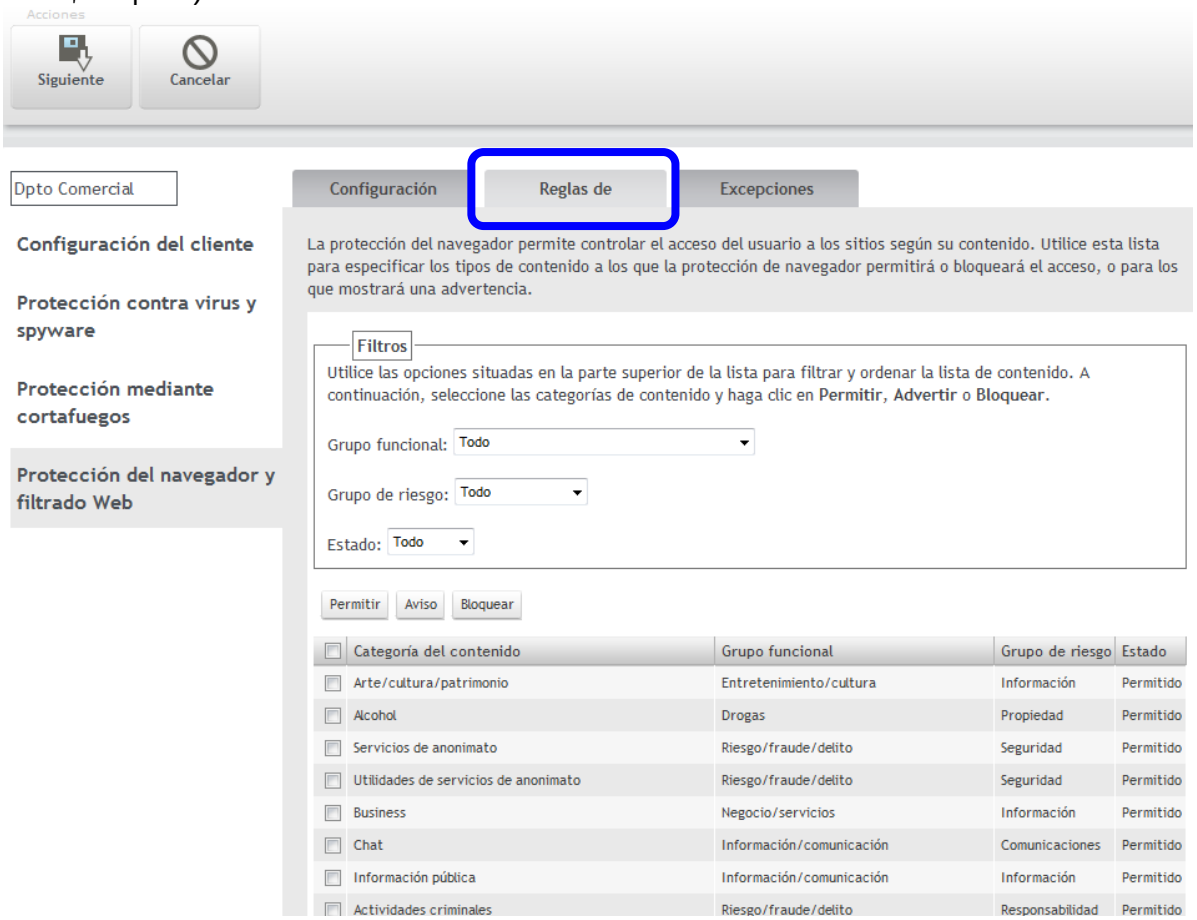
A continuación, podrá definir el nombre de la nueva directiva rellenando la casilla correspondiente. Haga clic en la pestaña “**Protección del navegador y filtrado web**”.


Panel
Equipos »
Informes »
Directivas
Acciones
Siguiente
Cancelar
Nueva directiva
Configuración del cliente
Configuración del cliente
Protección contra virus y spyware
Protección mediante cortafuegos
Protección del navegador y filtrado Web
Opciones de actualización
Comprobar si hay actualizaciones cada 24 horas
Actualizar equipos cliente en los que los usuarios no han iniciado sesión
Mostrar configuración
Especificar qué funciones del software cliente se va a mostrar en equipos cliente.
Visualización de la consola en equipos cliente:
Mostrar consola completa
Mostrar sólo resumen de estado
Mostrar sólo el icono
Ocultar la pantalla de bienvenida
Mostrar notificaciones de soporte en los equipos cliente

En el apartado "**Protección del navegador y filtrado web**", por defecto, aparece la pestaña "**Configuración general**" donde podrá configurar el nivel de acceso a sitios web y a las descargas de ficheros en función de su clasificación de seguridad general: "amarillo", "rojo" o "sin clasificar".


Acciones
Siguiente
Cancelar
Dpto Comercial
Configuración del cliente
Protección contra virus y spyware
Protección mediante cortafuegos
Protección del navegador y filtrado Web
Configuración
Reglas de
Excepciones
Dispone de licencias para el servicio de filtrado Web, pero puede que no esté instalado en todos los equipos. Compruebe que los equipos están ejecutando la última versión (5.0) en el informe Perfiles de equipos. Si los equipos no están ejecutando la última versión, deberá instalarla para que esta función esté disponible. Para ello, haga clic en Instalar protección.
Instalación automática
Instalar automáticamente la protección del navegador en todos los equipos que utilizan esta directiva
Cuando se selecciona esta opción, la protección del navegador se instalará en todos los equipos que utilicen esta directiva en la próxima comprobación de actualizaciones.
Acceso a sitios
Configure el acceso a los sitios en función de su clasificación de seguridad general.
Amarillo
Rojo
Sin clasificar
Acceso global al sitio:
Aviso
Bloquear
Permitir
Acceso a las descargas
Configurar acceso a descargas de archivos individuales basadas en su clasificación.
Nota: si se produce un error al bloquear descargas clasificadas como amarillas o rojas, se pueden introducir descargas de archivos peligrosas de sitios no autorizados.
Amarillo
Rojo
Sin clasificar
Acceso de descarga de archivo:
Permitir
Permitir
Permitir
Acceso a las páginas de phishing
Seleccione esta opción para bloquear todas las páginas de phishing.
Nota: cuando esta opción no está activada, los usuarios pueden acceder a páginas de phising conocidas en sitios autorizados.
Bloquear páginas de phishing

En la pestaña "**Reglas de contenido**", podrá configurar el nivel de acceso a los sitios web en función de su categoría de contenido. Por defecto, todas las categorías de contenido tienen estado "Permitido". Se puede cambiar el estado a "Bloquear" o "Aviso", seleccionando la/s categoría/s deseada/s, y a continuación, hacer clic en uno de los botones de estado (Permitir, Aviso, Bloquear).

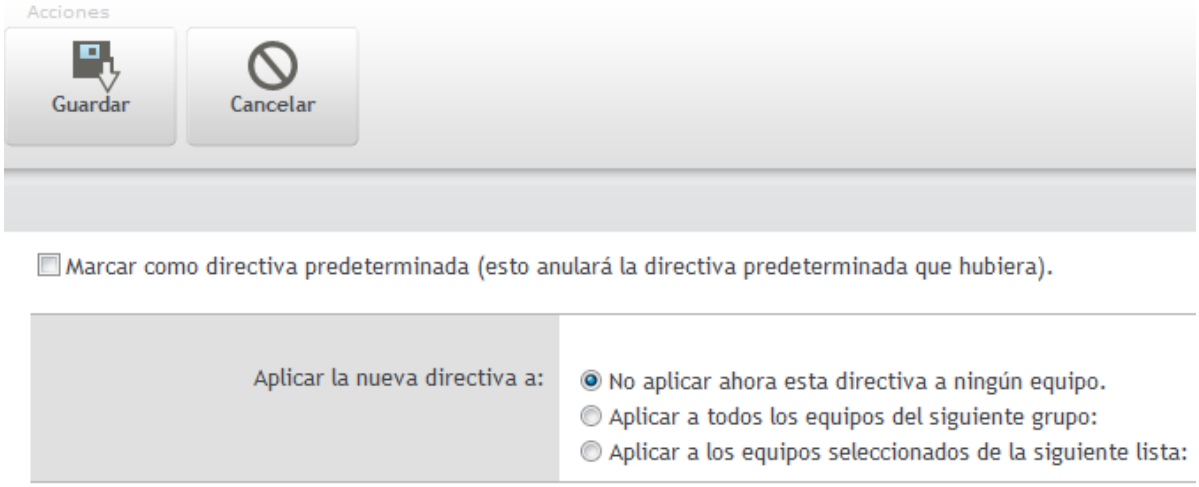


En la pestaña "**Excepciones**", se permiten agregar excepciones que prevalecen sobre las demás configuraciones de Filtrado Web.

Siguiente
Cancelar
Dpto Comercial
Configuración del cliente
Protección contra virus y spyware
Protección mediante cortafuegos
Protección del navegador y filtrado Web
Configuración
Reglas de
Excepciones
Lista de excepciones
La protección del navegador permite el acceso a los sitios autorizados y lo bloquea los sitios prohibidos que se indican a continuación. Introduzca una URL para cada sitio o un patrón de sitio para especificar un dominio o un grupo de sitios.
Agregar a lista de excepciones

Una vez personalizada la configuración de Filtrado web, haga clic en el botón "Siguiente" para aplicar la directiva de seguridad al/a los equipo/s.

En “Aplicar la nueva directiva a”, elija una de las 3 opciones. A continuación, haga clic en el botón “Guardar” para confirmarlo.


Acciones
Guardar
Cancelar
Marcar como directiva predeterminada (esto anulará la directiva predeterminada que hubiera).
Aplicar la nueva directiva a:
No aplicar ahora esta directiva a ningún equipo.
Aplicar a todos los equipos del siguiente grupo:
Aplicar a los equipos seleccionados de la siguiente lista:

Importante: La directiva no se aplica a los equipos de forma inmediata. Para forzar a que un equipo reconozca este cambio de directiva, deberá utilizar la opción “Actualizar ahora” en el icono de la Protección situado en la barra de tareas de Windows y/o reiniciar el equipo.

Centro de Seguridad.

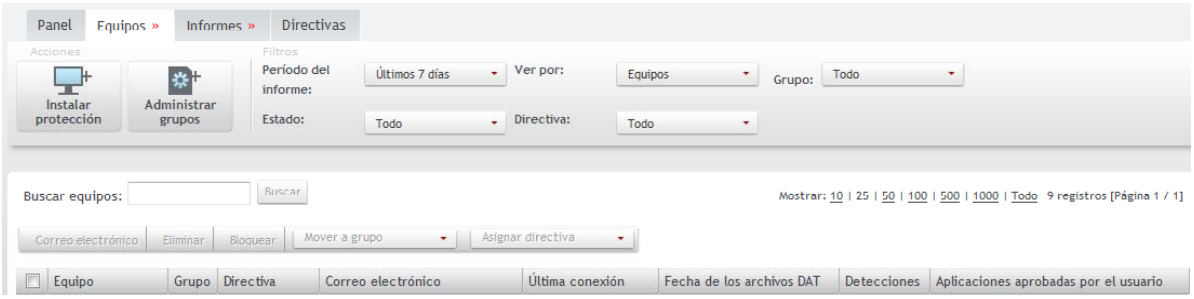
¿Qué tipo de información se puede obtener?

La pestaña principal **Informes** presenta 4 opciones:

Panel, **Equipos, Informes y Directivas**.

- Panel desglosa por grupos (creados por el usuario administrador) información sobre los equipos y licencias instaladas. En el apartado Cobertura indica licencias instaladas y No instaladas así como los equipos actualizados (los que han descargado la última actualización).

- Equipos. Esta opción permite:



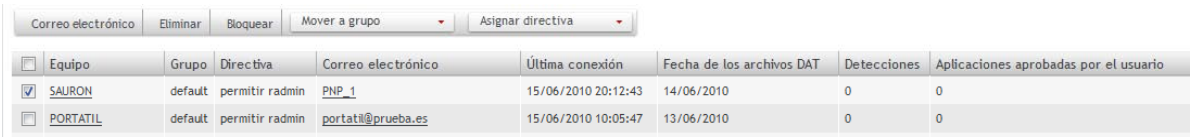
1. Encontrar algún equipo en concreto (introducir en "Buscar equipos" el equipo a buscar y aparecerá la información disponible).

2. Permite filtrar la lista de equipos con:

- **Ver por:** Equipos o Grupos.
- **Grupos**. Conjunto de equipos al que el usuario puede aplicar la misma política de seguridad. Facilitaría cualquier acción para el usuario pues si tiene 20 equipos y quiere aplicar a todos los mismos criterios, si no tuviese el grupo tendría que aplicar la directiva equipo a equipo.
- **Directiva** que se haya aplicado.

- **Periodos del Informe** de equipos en la última semana, o mes.
- **Estado** del equipo: Todos, No actualizados, aquellos que hayan tenido alguna detección en concreto, o equipos bloqueados.

3. Una vez se nos muestre la lista Equipos, y Seleccionando uno de ellos se puede:



- **Eliminar** el equipo. Se debe llevar a cabo sobre aquella máquina sobre la que se haya desinstalado el producto. Esta es la expresión técnica de lo que sería una reasignación de licencias por parte del Administrador, es decir, si el Administrador quiere reasignar las licencias adquiridas a PC´s distintos, sólo tendrá que desinstalar el producto de una de las máquinas, e instalarlo en la máquina nueva. En la siguiente comunicación la máquina aparecerá con la licencia asignada en el nuevo PC. Además, las actualizaciones del producto se realizarán a partir de ese momento sobre la nueva máquina.

- **Bloquear equipo**. Si, por ejemplo, no desea que realice actualización del producto instalado en el equipo.

- Incluir en algún **grupo.**

Pulsando sobre el enlace correspondiente al nombre de cada equipo aparece la información disponible de dicho equipo:

- **Detalles del equipo**:
  - Nombre del Sistema. Nombre del equipo.
  - Dirección de correo electrónico. La indicada en la instalación (modificable)
  - Grupo al que pertenece. Si no se indica ninguno pertenece el grupo establecido por defecto (modificable).
  - Directiva.
  - Protección contra virus y spyware .(Si lo tiene instalado).
  - Protección del Firewall. (Si lo tiene instalado).

- **Propiedades de equipo:**
  - Estado del equipo (Actualizado o No)
  - Última conexión con la plataforma (última conexión para descarga de actualizaciones para el producto)
  - Versión y Fecha del archivo DAT de firmas (última versión–actualización–descargada)
  - Idioma del producto.
  - Versión del motor (indica la versión de cada módulo de la protección instalada). Además, si no se encuentra actualizado, indica una serie de pasos para identificar el problema de las actualizaciones y solucionarlo.
  - Servidor de retransmisión. (nos indica si el equipo está configurado como tal)
  - Número de compilación de agente.
  - Número de compilación de analizador.
  - Versión del SO instalado en el equipo.
  - Versión del navegador de Internet Explorer instalado.

- **Dirección IP** del equipo.

- **Detecciones:**
  Informa (por períodos establecidos) de las detecciones así como de las aplicaciones aprobadas (permitidas) por el usuario y Sitios bloqueados.

Si se produce algún cambio (modificación de grupo, correo electrónico, etc...) deberá pulsar el botón guardar para aceptar los cambios.

- **Informes.** Esta opción permite al usuario ver informes de:

Centro de Seguridad
movistar
INFORMES
INSTALACIÓN
UTILIDADES
DESCONECTAR
Pack Seguridad
...¿necesitas ayuda?
Panel
Equipos »
Informes »
Directivas
Informes
Informes
Detecciones
Los tipos de amenaza y programas potencialmente no deseados encontrados en su red. Ordene la información de este informe por nombre de equipo o de detección y haga clic en una detección para leer una descripción detallada.
Perfiles del equipo
Información sobre el sistema operativo y la versión del navegador que utiliza cada equipo cliente de su red. Utilice este informe para localizar equipos en los que sea necesario instalar parches de software. Haga clic en un equipo para mostrar detalles adicionales.
Equipos duplicados
Equipos que aparecen más de una vez en los informes. Utilice este informe para localizar y eliminar instalaciones que no se usan en equipos obsoletos o en equipos en los que se volvió a instalar la protección.
Programas no reconocidos
Aplicaciones de Internet y/o programas potencialmente no deseados que se han detectado, pero aún no se han aprobado. Utilice este informe para identificar y controlar los programas que se ejecutan en su red y, a continuación, lleve a cabo adiciones a sus directivas.
Eventos entrantes bloqueados por cortafuegos
Comunicación entrante que la protección del cortafuegos personal ha impedido que acceda a su red.
Historial de detecciones
Gráficos que muestran el número de detecciones y de equipos donde éstas se han llevado a cabo cada mes del año pasado. Utilice este informe para evaluar el éxito de su protección y la estrategia de seguridad de su empresa.
Filtrado Web
Informe detallado con clasificaciones de los sitios Web a los que han accedido los equipos de su red. Utilice este informe para identificar los equipos que acceden a sitios Web de riesgo alto e implementar controles de acceso según las clasificaciones que hayan recibido.

- **Detecciones.** Muestra los resultados de todos los equipos, por grupos. Además por períodos de análisis, por tipo de detección y agrupar por equipo o detección. Muestra además los archivos detectados, la fecha de la última detección, grupo al que pertenece, etc...

- **Perfiles de equipo.** Muestra y organiza los equipos por sistema operativo y/o versión del navegador (Microsoft Internet Explorer).

- **Equipos duplicados.** Permite optimizar y actualizar la lista de equipos que por algún motivo hayan sido dados de baja, estén obsoletos o estuvieron protegidos y aquellos que lo están.

- **Programas no reconocidos.** Aplicaciones no reconocidas o certificadas por McAfee que pueden ser bloqueadas por el cortafuegos o potencialmente no deseados. Permite agruparlos por programas o por equipos.

- **Eventos entrantes bloqueados por cortafuegos.** La información es mostrada por períodos (última semana, mes, 3 meses y año) y se puede agrupar por equipos destino y equipos origen.

- **Historial de detecciones.** Muestra gráficos por mes y trimestre tanto de las detecciones encontradas como de los equipos con detecciones.

- Directivas. Permite crear tanto grupos como directivas. Inicialmente aparece la información de los grupos existentes con la directiva aplicada a cada uno.

Centro de Seguridad
movistar
INFORMES
INSTALACIÓN
UTILIDADES
DESCONECTAR
Pack Seguridad
...¿necesitas ayuda?
Panel
Equipos »
Informes »
Directivas
Acciones
Agregar Directiva
Directiva predeterminada:
McAfee Default
Nombre de directiva
Equipos
Acciones
McAfee Default
0
Ver directiva
ricardo
0
Editar | Eliminar | Copiar directiva
Aviso legal: La protección frente a virus y spyware está configurada de forma predeterminada para detectar programas potencialmente no deseados como, por ejemplo, el spyware. Seleccione si desea mantener o cambiar esta configuración de detección. En algunos casos, la eliminación de estos programas puede provocar que los programas host no funcionen correctamente, exigir que se desinstalen otros programas con acuerdo de licencia o requerir alguna otra acción por su parte.

Otras operaciones que pueden llevarse a cabo desde el Centro de Seguridad.

Las más importantes son las siguientes:

- Bloqueo/Desbloqueo de máquinas: Se consigue que la máquina bloqueada no se actualice. Se marcará en el check-box correspondiente para bloquearla o desbloquearla.

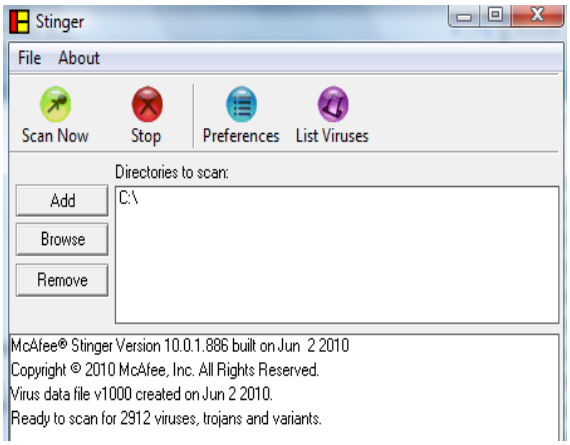
- Creación/Eliminación de un grupo: Los grupos permiten organizar la información para facilitar el uso del Administrador y realizar informes por grupos. Las máquinas podrán ser movidas de un grupo a otro para facilitar la administración. La eliminación del grupo debe ser posible sólo después de haber borrado todos los PC´s asociados.

6. Utilidades

¿En qué consisten? ¿Cómo funcionan?

Las herramientas son las siguientes:

1. **ContraVirus (Stinger).** Esta utilidad consiste en un escaneo que incluye troyanos y modificaciones que hayan podido tener éstos y los virus. El proceso es sencillo y tras la descarga o su ejecución en Internet simplemente hay que pulsar ***Scan Now***, realizando antes la selección de las unidades o carpetas que deseamos analizar.



2. **Diagnóstico (MER Tool)** o Herramienta de Escalación Mínima. Se trata de una opción del proveedor de software que permite compilar datos de la configuración del equipo.

Para usarlo hay que hacer clic en el enlace que nos solicitará que la aplicación pueda ser descargada en el PC o ejecutada desde Internet.

Se trata de 3 archivos donde aconsejamos abrir primero el archivo leeme.txt que incluye las instrucciones del proceso, entre ellas rellenar la hoja Excel donde hay que responder una serie de cuestiones sobre el PC, el sistema y también relativas a la Red de Área Local, equipamiento, etc... así como describir el problema.

Siguiendo las instrucciones del archivo de texto (5 pasos) llegamos a la última en la que se indica envíe por correo electrónico la información solicitada y puesta en formato .ZIP para ocupar el mínimo espacio posible.

3. **Desinstalador**. Esta utilidad permite buscar y eliminar componentes de Antivirus y/o Firewall de instalaciones anteriores que hayan quedado en el equipo garantizando una reinstalación de Antivirus y/o Firewall desde cero.